Abstract

The present invention discloses a general-purpose hierarchical key management method and apparatus whose trusted operation, with respect to compromise of keying material, does not depend upon the controlling application. This enables designs that separate secure key management from the application-specific use of the keying material, and enables the rigorous evaluation of the key management module.